IIS5 Security Best Practices (An Update!)

Michael Howard
Program Manager,
Security
Windows 2000 Team

Agenda

- The need for security
- Installation security best practices
- Web page and content development best practices
- Ongoing best practices

The Need For Security

- Web site attacks are at an all-time high
  - Defacements (data tampering threat)
  - Denial of service
  - Accessing confidential data (disclosure threat)
- #1 cause is administration oversight

Installation Security

- Install only what you need
- No samples
- No documentation
- No extra services
  - SMTP, NNTP, FTP, Index Server, Telnet

Installation Security

- Remove unneeded script maps
  - .htr, .stm, .printer, .ida etc
- Disable parent paths ('..')
- Disable IP address in content-location
  - Refer to Q218180

Content Development

- Many sites believe that adding a firewall makes them 'safe'
  - A great deal of traffic comes straight through port 80!
- It is imperative that your content be written securely and secured

User Input Is Bad!

- Do not trust user input
- Most of it is clean
- Some of it is malicious
- You must verify that all user input is valid
  - Especially if the data is used as input to a database, the file system or is presented back to other users

A Scenario

- Book company `A' allows you to post reviews
- Anyone can see a review
- An attacker posts the following review:

```
<meta http-equiv="refresh"
content="2; url=http://www.bookcompanyb.com">
```

- Any user looking at that book will be whisked away to book company `B'!

A Remedy

- Check all user input from FORMS and QueryStrings
- Use regular expressions
  - Use Visual Basic® Scripting Edition/ Jscript® v5 RegExp object

```
var reg = /<.*>/g;
if (reg.test(strInput)) {
        // Oh dear! HTML input!
}

var reg = /^[\s|\w|\.|\,|\'|\"|\;|\:\=]+$/g;
if (reg.test(strInput)) {
        // It's clean!
}
```

Don't Store Secrets!

- How many times have you seen this?

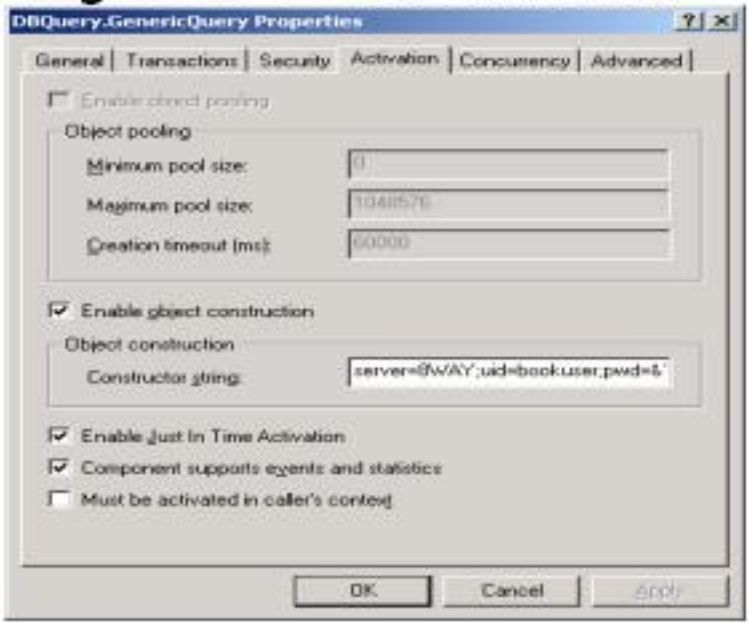
```
rs.Open "getBookList", _
"provider=SQLOLEDB;server=8WAY;" _
"initial catalog=booksales;" _
"uid=sa;pwd=$secret1;network=dbmssocn",0,1
```

- Don't store secrets in ASP!
- Consider obfuscating ASP code with the Microsoft® Script Encoder
  - Screnc.exe

Don’t Store Secrets!

- Access data through a custom COM+ object
- Use COM+ Explorer construction string
  - Refer to Q246138

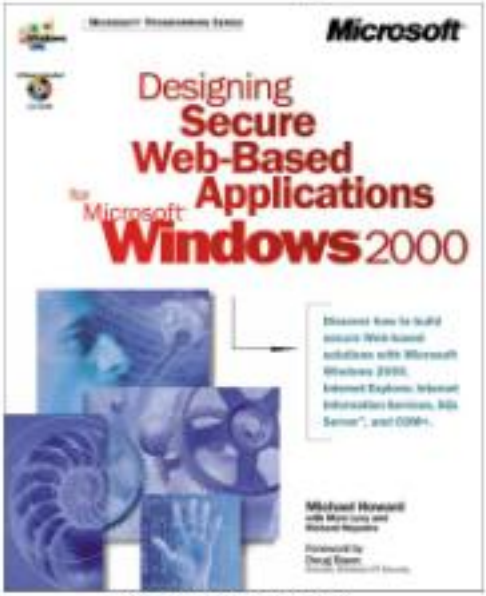
Using COM+ Construction



On-Going Security

- for (;;) {
  - Keep up to date with what's hot in security
    - http://www.microsoft.com/technet/security
  - Stay on top of fixes
    - Look at the Windows® 2000 IIS 5.0 Hotfix Checking Tool
  - Review checklists
  - Consider file integrity tools
    - Intact from www.pedestalsoftware.com
- }

Shameless Plug!



ISBN:0735609950

Summary

- The need for security
- Installation security best practices
- Web page and content development best practices
- Ongoing best practices